FORCEPOINT

Solution Brief

Forcepoint Behavioral Analytics

Executive summary

As the threat landscape continues to evolve, security leaders responsible for protecting data are turning to behavior analytics to prevent data exfiltration from accidental, malicious, and compromised users. Forcepoint Behavioral Analytics is a powerful behavior analysis platform that enables security teams to proactively monitor for high risk behavior.

Forcepoint's market-leading solution integrates structured and unstructured data to provide holistic visibility into nuanced human activity, patterns, and long-term trends that comprise human risk. The product offers a variety of customer use cases through a diverse set of analytics built upon four tenets: Diverse Data Sources, Hybrid Analytics, Configurability, and Transparency.

1.) Diverse data sources

Forcepoint Behavioral Analytics is a powerful platform with a defined generic data model, flexible enough to handle incredibly diverse data yet structured enough to apply powerful big data analytics. The product's information model provides specific guidelines for how to map data from different sources in order to maximize the effectiveness of the analytic engines.

- The flexible data model, in combination with the detailed information model, enables security operation operatives and analysts to integrate existing and future security products without the need for new product releases or data scientist intervention.
- Organizational data sources such as data loss prevention (DLP) tools, security information and event management (SIEM) tools, and even HR applications are examples of relevant data sources (see Figure 1).
- Traditional behavioral analytics platforms integrate with a static set of data sources. Updates to these platforms require downtime and the expertise of engineers and data scientists.

Benefit

Comprehensive Visibility

Forcepoint is the only vendor that covers structured and unstructured business data in addition to communications to leave no detection gaps.

Figure 1. Examples of Behavioral Analytics ingest sources

2.) Hybrid analytics

Traditional security approaches are rule (policy) driven, with hundreds, thousands, or even tens of thousands of pre-defined patterns used to identify known bad activity. Such rule-based approaches are attractive because they allow experts to encode knowledge about specific bad activities, yet are limited in their effectiveness.

When new threats emerge, users must act quickly to create corresponding policies. Additionally, policy- or rule-based approaches are not able to detect subtle, risky behavior. For example, if a person logs in from an unusual location and copies sensitive documents they haven't recently accessed, this may constitute risk even if it doesn't violate a policy. Forcepoint Behavioral Analytics employs both rule-based and statistical disciplines by combining the two into a hybrid analytic approach that is far more effective than either approach alone.

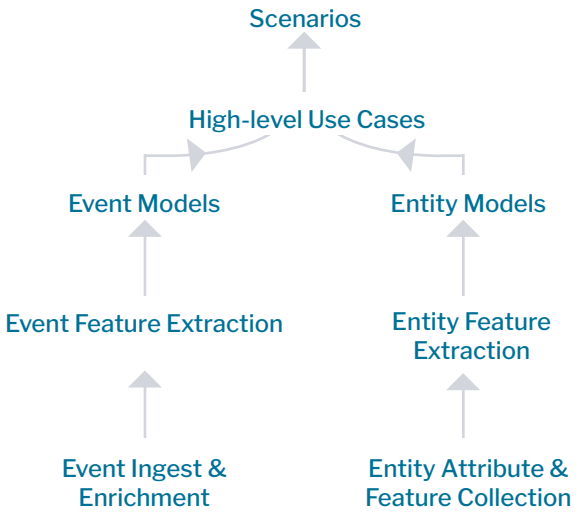

Figure 2. Forcepoint Analytic Hierarchy

Forcepoint's Analytic Hierarchy (shown in Figure 2) is made up of features, models, and scenarios:

- Features are bits of information extracted from individual events that may make a person or their activity interesting: they can represent behavioral patterns (e.g., the hour of day, destination domain, or applications used); they may be related to data characteristics (e.g., file type, file size, classification, or sentiment); they may be person-specific (e.g., role, office location, administrative access privilege levels, or results from a performance review). Forcepoint's solution automatically learns the distribution of feature values across event datasets, which enables it to use artificial intelligence approaches to recognize anomalies and calculate risk.
- Features are used to define models, which are also statistical- and data- driven. Models compute summary statistics to describe an entity's activity over time. Forcepoint's models are unique in that they provide either partial or, in some instances, full access to the underlying analytics and engine. A model may measure, for example, the number of bytes uploaded to a cloud storage site, the number of unique printers accessed, or how anomalous a user's web search activity is relative to his or her own past or against an organizational baseline. All raw model scores are normalized with respect to prior observations, and users or analysts can utilize their learned expertise of the organization.
- Finally, scenarios correspond to high-level use cases and consist of several models. One example is the Data Exfiltration scenario, which combines a variety of model scores that may indicate an employee is leaking data.

Benefit

Deep Context

Focus on behaviors, not just anomalies, with precise narratives that indicate unwanted behavior.

3.) Configurability

Not only does Forcepoint Behavioral Analytics use a hybrid approach to analytics, effectively combining domain expertise with the power of artificial intelligence, but the encoding of domain expertise is exposed to all administrative users. Forcepoint sets itself apart from competitors in that it allows application end-users or analysts to contribute their own domain expertise about their organizations, their data, and their people. Security risks vary widely across organizations, depending on the industry, region, and standard business practices. Raw event model scores contributing to an entity scenario's risk score are shown on an entity timeline and the events that contribute the most to those model scores are shown clearly. Forcepoint empowers security operations analysts to contribute their own expertise to build their own use cases, manage and build their own analytics, and develop analytical use cases without the help of engineering or support service groups. Users may configure and tune additional features, models, or scenarios all through the user interface. (Figure 3) Lexicons allow customers to easily customize and manage keywords and phrases such as project code names. Customers also have the flexibility to enable additional privacy controls for lexicons deemed highly confidential to certain business units such as HR or Legal.

Benefit
Flexibility Easily build or customize risk models to fit any unique organization and support any risk use case.

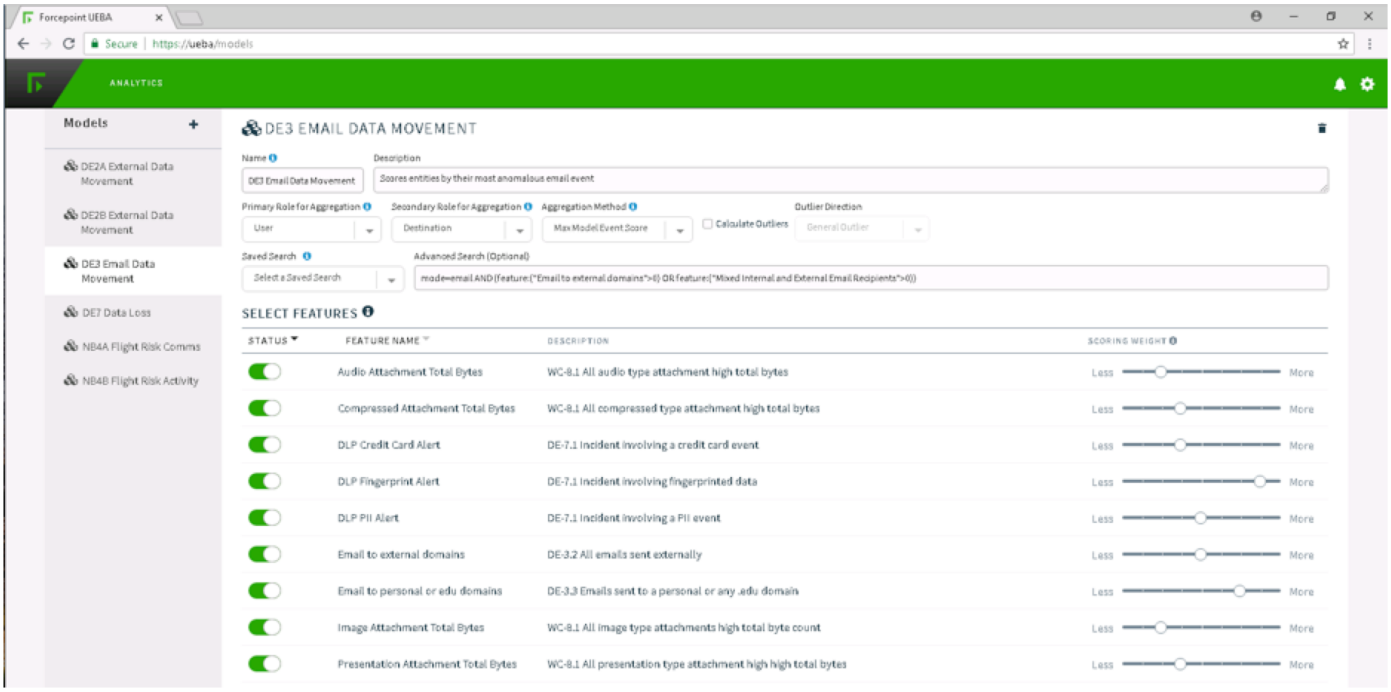

Figure 3. Flexible data model tuning and configurability

4.) Transparency

The analytics in Forcepoint Behavioral Analytics are simple and easy to understand, producing accurate and insightful results. Unlike competitor products, Forcepoint Behavioral Analytics provides transparency by exposing enhanced detail so analysts can understand how the user community works and then add their own expertise to the features and models. For example, an analytics administrator can change the scoring weight of a cloud storage upload or weekend activity based upon the data feeds from various data sources, such as the organization's SIEM or DLP tool set. When the analyst investigates a user of interest, they do so through the user-friendly entity timeline, which provides analytic explanations and context, allowing the analyst to make informed judgments and take appropriate actions as they assess possible security threats (Figure 4).

Benefit

Efficiency

In-depth analytics within a single platform allows investigators to pivot from alert to investigation.

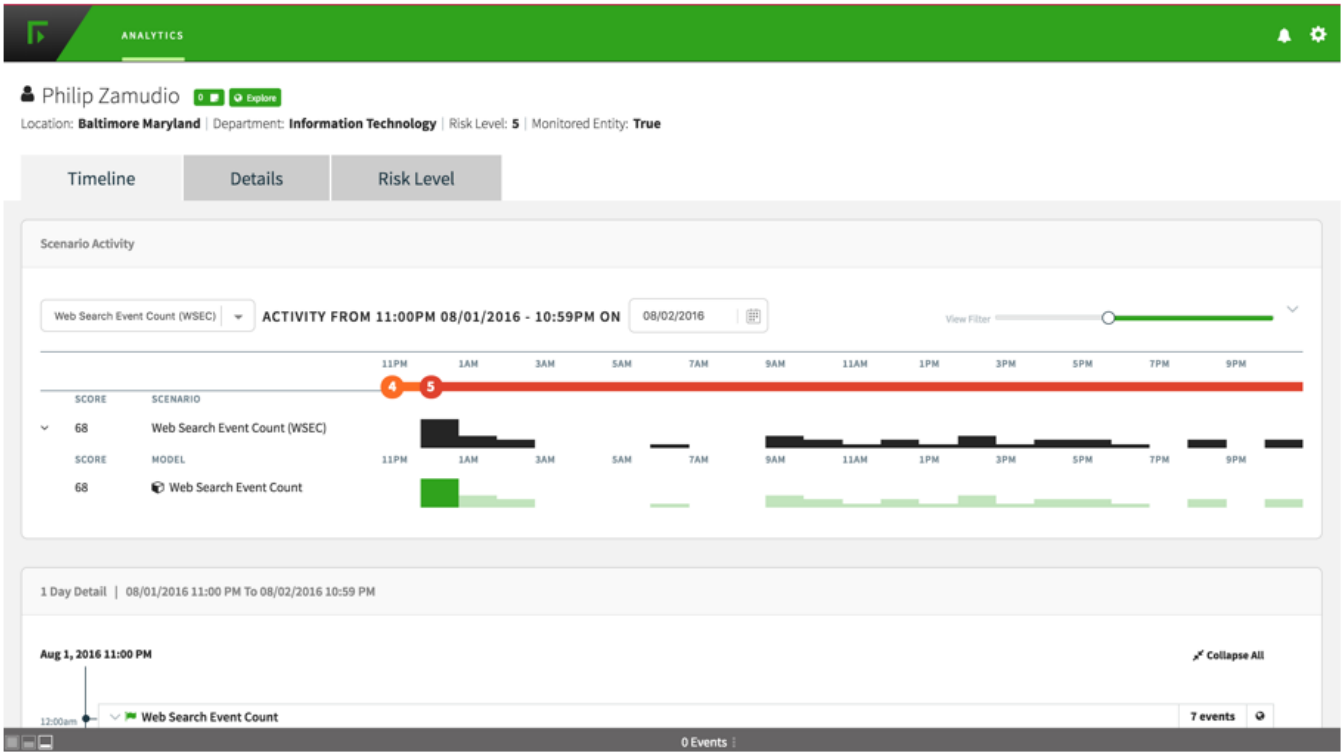

Figure 4. An end-user's risk score as shown on the entity timeline

Summary

Organizations want to avoid data security incidents to stay out of the headlines, and therefore choose behavior analytics to protect data from accidental, malicious, and compromised users. Forcepoint Behavioral Analytics protects sensitive client information, detects compromised accounts, and enforces the continued improvement of an organization's internal security culture.

Organizations that choose Forcepoint to improve their security posture gain many benefits, including:

- **Comprehensive visibility ›** Forcepoint is the only vendor that covers structured and unstructured business data in addition to communications to leave no detection gaps.
- **Deep context ›** Focus on behaviors, not just anomalies, with precise narratives that indicate unwanted behavior.
- **Flexibility ›** Easily build or customize risk models to fit any unique organization and support any risk use case.
- **Efficiency ›** Pivot from alert to investigation with in-depth analytics within a single platform.

To learn more, visit:
forcepoint.com/behavioralanalytics

forcepoint.com/contact